International Journal of Information Security (2024) 23:1603–1618
https://doi.org/10.1007/s10207-024-00812-4

REGULAR CONTRIBUTION

From sinking to saving: MITRE ATT&CK and D3FEND frameworks for maritime cybersecurity

Awais Yousaf[1] · **Jianying Zhou**[1]

Published online: 19 January 2024
© The Author(s), under exclusive licence to Springer-Verlag GmbH, DE 2024

Abstract
Cybersecurity is a growing concern for maritime sector. Modern ships are practical realism of cyber physical systems that utilize both information technologies and operational technologies. Cybersecurity incidents on such systems require robust and explainable models that should provide deep insights about the nature of an attack. Many frameworks for modeling of cyber attacks exist, but they cover only the tiny part of modern multidimensional attack surfaces. MITRE ATT&CK is the most comprehensive cyber attack modeling framework that covers the multidimensional nature of modern cyber attacks. MITRE D3FEND is similar to ATT&CK knowledge base, but it represents cyber defense framework. In this paper, we aim to demonstrate the modeling with MITRE ATT&CK and MITRE D3FEND frameworks for maritime cybersecurity. An attack scenario against ballast water management system of the ship is considered and modeled with the help of ATT&CK. Moreover, two defensive mechanisms are suggested. First is created with the help of D3FEND framework and second leverages the strength offered by mitigation techniques of ATT&CK. We believe that the demonstration of MITRE ATT&CK and D3FEND frameworks for modeling of maritime cyber attacks and maritime defense, respectively, would pave the way for the development of future maritime cybersecurity solutions.

Keywords Maritime cybersecurity · MITRE ATT&CK · MITRE D3FEND · Information technology · Operational technology

1 Introduction

Traditional ships are simple, and their functional components operate independent of each other. Trends in ship building have moved significantly from traditional ships to semi-autonomous and autonomous ships that perform many intelligent operations, e.g., autonomous navigation and route planning without the intervention of a captain or crew. International Maritime Organization (IMO) has defined the four levels of autonomy for autonomous ships [1, 2] and depending upon the level of autonomy used, sometimes there are no seafarers required on board the ship. Few examples of commercial autonomous vessel projects are Wartsila's IntelliTug [3], YARA Birkeland [4], L3Harris maritime autonomous systems [5] and Japan's fully autonomous ship program MEGURI2040 [6]. Few names in academia that are under active research in the domain of maritime autonomous shipping and maritime cybersecurity are Cetus project [7] by University of Plymouth (UK), milliAmpere-II Autonomous Passenger Ship (APS) under Autoferry Project [8] by Norwegian University of Science and Technology (NTNU). As ships are sailing through the journey toward autonomy, they have more interconnected devices and connectivity with the cyber world, which provides more attack surface for the malicious actors of the cyber world.

Broadly, navigational bridge systems, communication systems, engine control systems and stability systems are crucial parts of a ship for its daily operations [9]. Navigational bridge systems include Electronic Chart Display and Information System (ECDIS), Radio Detection and Ranging (RADAR), Automatic Identification System (AIS), Global Positioning System (GPS) and Dynamic Positioning System (DPS). Communication systems include satellite communication system, Voice over Internet Protocol (VoIP) phones and wireless local area network. Engine control systems include engine, fuel tanks, programmable logic controllers

✉ Awais Yousaf
awais_yousaf@sutd.edu.sg

Jianying Zhou
jianying_zhou@sutd.edu.sg

[1] iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design (SUTD), Singapore, Singapore

(PLCs) and a lot of sensors and valves. Similarly, stability systems manage the stability of a ship with the help of Ballast Water Management System (BWMS). BWMS consists of large tanks that are positioned at the bottom of a ship as well as on the left and right sides of the hull. These tanks can be filled or emptied via PLC connected ballast pumps that can be controlled via human–machine interface (HMI). All the crucial parts of the ship are connected with each other for smooth and safe sailing of a ship.

Historically, many cyber threat modeling frameworks have been developed in concurrence with increased dimensionality and complexity of cyber attacks. The old CIA triad of confidentiality, integrity, and availability is a popular framework for Information Technology (IT) that has been used for many years. Main issue with CIA is that it only covers three dimensions (confidentiality, integrity, and availability) of cyber incidents. Tree-like structures like attack trees [10] and threat trees [11] have also been used for cybersecurity modeling but fundamental issue with these structures is that they are unable to model interlinked nature of multistage attacks. They mainly cover only one dimension depending upon the nature of the attacks. Lockheed Martin introduced Cyber Kill Chain (CKC) framework which comprises of seven phases of modeling, namely Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives. CKC is a chain because if any phase of the attack is blocked or failed then the consequence is the failure of the overall attack [12]. Similarly, STRIDE which is an abbreviation of Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege is another threat modeling framework developed by Microsoft. STRIDE covers more dimensions as compared to CIA, which only covers three [13, 14]. Most comprehensive and robust cyber attack modeling framework is MITRE ATT&CK. (Details of which are provided in Sect. 2.) Main advantage of MITRE ATT&CK framework is that it is useful for the modeling of modern multidimensional and interlinked nature of maritime cyber attacks. It provides coverage for IT infrastructure as well as for Operational Technology (OT) and mobile infrastructures.

A lot of effort has been put for designing of cyber attack frameworks but efforts for cyber defense frameworks are apparently not significant. In [15], a simple defense modeling is performed with the help of Defense Trees (DTs) which are simple extension of attack trees. DTs are constructed by adding mitigation techniques as the leaf nodes of the attack trees. An improvement for DTs is proposed in [16] in the form of Attack-Defense Trees (ADTrees). In ADTrees, two types of nodes are defined namely attack nodes and defense nodes. Unlike DTs, any node of ADTrees can have one child node of opposite type as an optional node representing the countermeasures. Similar to ADTrees, Attack Countermeasures Trees (ACT) are proposed in [17] but unlike DTs, multiple countermeasure nodes can be placed at any node of the tree. Moreover in ACT, detection and mitigation techniques are treated separately. Tree-like structures can be useful for analytical evaluation of success of cyber attack or defense, but they do not provide enough insights for the development of effective and robust cybersecurity solutions. For better insights and coverage, MITRE ATT&CK framework provides mitigation techniques for each of its attack techniques that can be used to model the cyber defense (Sect. 6.2). Moreover, MITRE has also developed D3FEND framework [18], which is most comprehensive cyber defense modeling framework and is similar in architecture to MITRE ATT&CK framework (Sect. 6.1). Attack and defense modeling frameworks are summarized in Table 1.

Table 1 Summary of different frameworks

Attack Modeling	Defense Modeling
Attack Trees	Defense Trees
CIA	Attack-Defense Trees
STRIDE	Attack Countermeasure Trees
Cyber Kill Chain	ATT&CK Mitigation
MITRE ATT&CK	MITRE D3FEND

Rest of the paper is organized as follows: Section 2 briefly explains MITRE ATT&CK and MITRE D3FEND frameworks. Section 3 discusses related work in the field of maritime cybersecurity. Section 4 highlights the main motivations and contributions. Section 5 discusses maritime attack on a ship in details. Modeling of maritime attack with MITRE ATT&CK framework is also presented in this section. Section 6 has two subsections and proposes a defense for a ship considered in Sect. 5. Defense is modeled with MITRE D3FEND in Sect. 6.1, whereas it is elaborated with the help of ATT&CK mitigation techniques in Sect. 6.2. Moreover, key findings, strengths and limitations of this work are discussed in Sect. 7. Some thoughts on future work are also provided in this section. Finally, the conclusions are drawn in Sect. 8.

2 MITRE ATT&CK and D3FEND frameworks

Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) by MITRE Cooperation is a globally accessible knowledge base of adversary behavior. It is a threat modeling framework commonly useful for Cyber Threat Intelligence (CTI). MITRE ATT&CK framework helps modeling cyber attacks by providing three matrices, namely *enterprise* for Information Technologies (IT), *Industrial Control System* (ICS) for Operational Technologies (OT) and *Mobile* for mobile technologies. All matrices have similar layout. First

row lists Tactics that represent the objectives of an attacker. Under each Tactic, a column of Techniques is provided. Techniques represents attacker's way of realizing a Tactic. Apart from Tactics and Techniques, MITRE ATT&CK framework also provides information about data sources, platform, software, mitigation and detection schemes for each technique. Such a huge availability of information aids in capturing the granular details of actions (Techniques) that an attacker can use to accomplish his motives (Tactics).

MITRE ATT&CK framework has 14 Tactics each for Enterprise Matrix and Mobile Matrix, whereas 12 Tactics are available for ICS Matrix. In this paper, mobile matrix is not considered as ships are mostly composed of IT and ICS infrastructure. Moreover, cybersecurity of broadband communication link between ship and Shore Control Center (SCC) is beyond the scope of this work. Tactics along with their IDs for Enterprise and ICS matrices are tabulated in Table 2. At the time of writing this paper, there are 193 techniques and 401 sub-techniques available in Enterprise whereas 79 techniques are mentioned for ICS [19].

MITRE D3FEND is similar ontology as MITRE ATT&CK. This framework establishes a granular semantic model of countermeasures, their properties, relationships and history of development [18]. Defensive cybersecurity countermeasures are used to negate or offset offensive cybersecurity activities. MITRE D3FEND development is based on cybersecurity patents (United States Patent Office filings from 2001 to 2019), MITRE Cyber Analytic Repository [20], academic papers, engineering journals, technical specifications and publicly available technical documentations. MITRE D3FEND is a knowledge base and critical counterpart of MITRE ATT&CK. D3FEND and ATT&CK, both are encoded via Structured Threat Information eXpression (STIX) [21] based standard of Organization for the Advancement of Structured Information Standards (OASIS). Moreover, like MITRE ATT&CK, MITRE D3FEND framework has defensive Tactics and Techniques.

As explained in [18] and shown in Fig. 2 [22], first row of D3FEND framework represents defensive tactics, second row symbolizes base techniques and remaining rows are defensive techniques that varies from more general usage to more specific usage with respect to the increasing order of rows (Fig. 2). Secondly, all (rows three and onward) techniques are based on the base technique (second row). Lastly, as self-explanatory from Fig. 2, a defender cannot *Evict* an attacker if he cannot *Detect* the attacker, and he cannot *Detect* the attacker if it is not there. Ideally, the defender would *Harden* his environment before the attacker penetrates it [18].

3 Related work

Maritime safety is the oldest concern of IMO regulations [23]. After unfortunate incident of Titanic ship, Safety Of Life At Sea (SOLAS) Convention was adopted in 1914 and after multiple updates, current version of SOLAS was adopted in 1974 [24]. It is the most important convention of IMO for maritime safety. Originally, SOLAS focused on the safety of the ships, it did not address the security issues of the ships and ports. Later, SOLAS two codes namely International Safety Management Code (ISM Code) and International Ship and Port Facilities Security Code (ISPS Code) inadequately covered few aspects of security for ships and ports. Because maritime cybersecurity is a grue-

Table 2 MITRE ATT&CK framework

Enterprise ID	Enterprise Tactics	ICS ID	ICS Tactics
TA0043	Reconnaissance	TA0108	Initial Access
TA0042	Resource Development	TA0104	Execution
TA0001	Initial Access	TA0110	Persistence
TA0002	Execution	TA0111	Privilege Escalation
TA0003	Persistence	TA0103	Evasion
TA0004	Privilege Escalation	TA0102	Discovery
TA0005	Defense Evasion	TA0109	Lateral Movement
TA0006	Credential Access	TA0100	Collection
TA0007	Discovery	TA0101	Command and Control
TA0008	Lateral Movement	TA0107	Inhibit Response Function
TA0009	Collection	TA0106	Impair Process Control
TA0011	Command and Control	TA0105	Impact
TA0010	Exfiltration	–	–
TA0040	Impact	–	–

some reality today, the Maritime Safety Committee (MSC) of IMO, at its 98th session in June 2017 has adopted a Resolution MSC.428(98)—Maritime Cyber Risk Management in Safety Management Systems [25]. The resolution encourages administrations to make sure that existing safety management systems (as defined in the ISM Code) adequately address cyber risks no later than the first annual review of the business's Document of Compliance (DOC) after January 1, 2021.

Like the developments happening at IMO, specially the Resolution MSC.428(98) which has been imposed to in-service maritime vessels since the start of January 2021, International Association of Classification Societies (IACS) has adopted two new Unified Requirements (URs) [26] known as cyber resilience of Ships (E26) and cyber resilience of onboard systems and equipment (E27). Both URs will be the mandatory requirements for the ships contracted for construction on or after 1st of January 2024. Both URs highlight the common set of minimum functional and performance requirements for a ship and its OT and IT systems and these requirements are necessary for a ship to be cyber resilient.

Since the adoption of resolutions and many initiatives taken by IMO for maritime cybersecurity and related legal instruments, lot of research has been conducted for maritime cybersecurity. Recently, researchers have started adopting MITRE ATT&CK framework for modeling of maritime cyber attacks but usage of MITRE D3FEND for modeling of maritime defense is rather rare. Research works mentioning D3FEND are given in [27–31], but these works are not related to maritime defense. To the best of our knowledge, adoption of MITRE D3FEND for maritime cyber defense is missing in the literature.

In [32], an attack on software of ECDIS is demonstrated. Attack is executed using a malware that functions as a Man in The Middle (MiTM) for intercepting and tampering of the incoming GPS coordinates. Moreover, malware is capable to crash the Operating System (OS) of crew workstation on which the ECDIS is installed. Crew workstation is normally considered as air-gapped which means it is not connected to the internet. Therefore, malware is delivered via exfiltration over USB attack (ATT&CK ID: T1052). The goals of the malware are dual. First, it misguides the ship by compromising the integrity of GPS coordinates and then after a delay, it crashes the OS by provoking the blue screen. Although authors of the paper nicely demonstrated the cyber attack on ECDIS but as usual, cyber attack modeling with standard attack modeling framework like MITRE ATT&CK is missing.

Attacks related to the integrity of Integrated Navigation System (INS) and ECDIS are summarized in [33]. Like [32], tampering of GPS coordinates is performed with the help of malicious USB device. It is demonstrated that the received GPS coordinates available in Sensor Integrator (SINT) unit [32, 33] can be modified. In the second approach demonstrated for GPS tampering, SINT is overridden with the help of a small computer like Raspberry Pi which is connected to a network switch in INS network. Moreover, cryptographic countermeasures are explained to mitigate the effects of demonstrated attacks. Authors gained all the information related to INS and its vulnerabilities through internet searches. Like [32], cyber attack modeling with standard attack modeling framework like MITRE ATT&CK is missing. Moreover, countermeasures adopted for defense are not mapped to D3FEND framework.

Security vulnerability assessment is performed for three different ECDIS systems, namely Transas Navi Sailor 4000, Navi Sailor 4000 and NACOS MULTIPILOT Platinum 2017 in [34–36], respectively. For all three ECDIS systems, remote code execution vulnerability is identified in both Remote Desktop Protocol (RDP) and Server Message Block (SMB) with the help of NESSUS vulnerability scanning tool [37]. Like [32, 33] knowledge base like ATT&CK is not used for modeling of maritime cyber attacks.

Feasibility of AIS as a covert channel is analyzed in [38]. AIS is analyzed to determine the extent to which it can be useful for an attacker to achieve his objectives (ATT&CK Tactics). Two cyber kill chains are considered. In first kill chain, AIS is controlled with the help of a small computer (like Raspberry Pi) running a script on Kali Linux virtual machine, whereas, in second kill chain, a USB stick is used to load the malware into the system for controlling of AIS. Unlike [32–36], both kill chains are well described with the help of MITRE ATT&CK framework.

In [39], a maritime cyber risk management framework is presented. This framework comprises three main steps, namely assessment preparation, assessment conduct and results communications. In the first step, different cyber systems of the ship are classified using technical specification sheets of each system. In the second step, expert opinions are sought on the outputs of the first step. Then, computational vulnerability scanning tool is used to identify the weaknesses and vulnerabilities in the cyber systems of the ship. Finally, risk matrix-based approach [9] is used to quantify the risk in third step. After the second step, authors identify different weaknesses and vulnerabilities, but they do not use the standards like MITRE Common Weakness Enumeration (CWE) [40] and Common Vulnerabilities and Exposures (CVE) [41], which are considered standards among cyber security pundits.

Another risk assessment framework is proposed in [42] for autonomous passenger ship. This framework heavily relies on Failure Modes Effects and Criticality Analysis (FMECA) [43], and unlike [39], it uses MITRE ATT&CK framework. FMECA is a design-level process, which consists of three main phases. In each of the phases, ATT&CK framework helps FMECA by providing granular details of the cyber

attacks with the help of MITRE ATT&CK tactics and techniques. After demonstrating the effectiveness of proposed risk assessment framework, Integrated Navigation System (INS) is considered in [44] as a test case for the evaluation of proposed risk assessment framework. As discussed above, ATT&CK is not a risk assessment framework, but it can be used in conjunction with other standards and procedures for the development of risk assessment frameworks and cybersecurity solutions.

4 Motivation and contributions

Existing cyber threat modeling frameworks have been actively used but serve different purposes and have specific use cases in the field of cybersecurity. For example, STRIDE is used to categorize and prioritize threats; CKC framework analyzes the stages of a cyber attack to understand and get better insight for each stage. Similarly, tree-based frameworks [15–17] help visualizing attack and defense paths, making the analysis easier for cybersecurity solutions. All these frameworks are theoretically or empirically established and have proper definition and structure. Contrary to this, MITRE ATT&CK and D3FEND frameworks are truly based on real-time cybersecurity incidents and observations and therefore have more practicality from cybersecurity perspective. Hence, MITRE ATT&CK and D3FEND frameworks are chosen for demonstration of their usability for maritime sector due to their intrinsically realistic nature. To the best of our knowledge, a combined study that jointly models maritime attacks and defenses with MITRE ATT&CK and MITRE D3FEND, respectively, is not available in the literature.

MITRE ATT&CK framework deals with IT, OT and mobile systems with its respective matrices, but none of the ATT&CK matrices are specific to maritime sector. For a navigational bridge of a ship, notable OT systems are GPS, AIS, RADAR and ECDIS. Detailed example of an attack on AIS is given in [38], whereas attacks on ECDIS are discussed in [32–36]. Similarly, attacks on maritime RADARS are executed in [45, 46]. There is not a single entry in all three ATT&CK matrices that mentions any single attack technique for systems like ECDIS, RADAR and AIS. Few examples are available in MITRE ATT&CK for GPS, but they are not related to maritime sector. In this work, we have demonstrated the applicability of MITRE ATT&CK matrices for maritime sector. Although there are some limitations but for sake of conciseness, the proposal of new ATT&CK like matrix for maritime sector is left for future work (Sect. 7.3).

MITRE ATT&CK has widespread adoption, but its application within the maritime domain is notably rare. Most of the works mentioned in Sect. 3 have not utilized ATT&CK framework for modeling of maritime cyber attacks. For example, cyber attacks are well demonstrated on ship systems [32–36, 47] but are not modeled with ATT&CK. To some extent, ATT&CK is utilized to model CKC in [38] for AIS system only. In this work, whole ship is explored as an attack surface in contrast to earlier studies in which only one system or subsystem is considered for demonstration of attacks. Unlike MITRE ATT&CK, MITRE D3FEND does not have widespread adoption. Research works mentioning D3FEND are given in [27–31], but these works are not related to maritime sector. To the best of our knowledge, adoption of MITRE D3FEND for maritime cyber defense is missing in the literature.

Traditionally, defense modeling has been performed with DTs [15], ADTrees [16] and ACTs [17]. These tree-based approaches are well known and have a history of usage and reliability. From defense perspective, there are two possibilities. In one situation, attack happens and based on the analysis of the attack, we incorporate a mitigation technique in the system. On the other hand, attack information may not be known a priori. In the former situation, mitigation techniques can be chosen from ATT&CK knowledge base, but in the later scenario, MITRE D3FEND is more suitable when the attack vector is unknown. To the best of our knowledge, design of maritime defense by D3FEND in case of unknown attack vector is not available in the literature.

Lastly, in this work, an amalgamated research is performed from cyber attack and cyber defense perspectives. Traditionally, cyber attacks have been discussed in the literature along with some suggestions for their countermeasures. In contrast, a detailed cyber attack vector is explored in this work for BWMS, considering the whole ship as an attack surface and then suitable countermeasure techniques are provided from ATT&CK mitigations. Additionally, defense with D3FEND is designed for same ship when a priori knowledge of attack vector is considered hidden or unspecified. As explained in the subsequent sections, cybersecurity concepts applied for BWMS can be extended for the rest of the systems onboard ship.

5 Maritime attack

A ship is an ICS that consists of IT and OT networks. Ship BWMS is an OT network which is connected behind IT network and ship IT network is connected to the satellite communication system. Satellite communication system is used to communicate to Shore Control Center (SCC). Ships can communicate to SCC via satellite communication system only if they are in the open sea. Depending upon the level of autonomy used [1, 2], a ship may need to provide partial or full control of the ship as well as it also sends statistics about performance parameters of shipboard systems (including BWMS) to SCC; therefore, it is more vulnerable to cyber attacks. In this section, a scenario of sinking of a ship is con-

Table 3 MITRE ATT&CK Reconnaissance (TA0043) techniques

Technique ID	Technique for Reconnaissance
T1589	Gather Victim Identity Information
T1590	Gather Victim Network Information
T1592	Gather Victim Host Information
T1593	Search Open Websites/Domains
T1594	Search Victim-Owned Websites
T1595	Active Scanning
T1596	Search Open Technical Databases
T1598	Phishing for Information

Table 4 MITRE ATT&CK Resource development (TA0042) techniques

Technique ID	Technique for Resource Development
T1583	Acquire Infrastructure
T1584	Compromise Infrastructure
T1586	Compromise Accounts
T1587	Develop Capabilities
T1608	Stage Capabilities
T1650	Acquire Access

sidered by attacking its BWMS and this scenario is modeled with MITRE ATT&CK framework.

Secret study on how a cyber attack could be used to sink a cargo ship or blow up a fuel pump at a gas station is revealed in classified documents, which are reportedly from Iran [48]. Leaked documents reveal how a ship's BWMS can be used as a target to sink a ship. According to IMO convention for the control and management of ship's ballast water and sediments [49], BWMS is mandatory for a ship to avoid spread of harmful and invasive aquatic species to marine environment near shores. It is also required to maintain the balance and center of gravity of the ship. It is a large tank that is positioned at the bottom of a ship as well as on the left and right sides of the hull. Ballast water can be pumped to and from the ballast tank via PLC connected ballast pumps that can be controlled by HMI.

Consider that cyber attack starts with ATT&CK Tactic called Reconnaissance (TA0043). Main objective here is to gather as much information of the target vessel as possible. For this purpose, ATT&CK techniques mentioned in Table 3 can be used:

Initially, techniques T1589, T1590 and T1592 can be used to collect information about victim identity, network and host, respectively. Gaining of personal information such as crew names, email addresses as well as sensitive information like password credentials (sub-technique T1589.001) is the main requirement of T1589. Information about networks may contain a range of administrative data such as IP ranges and domain names as well as information about network topologies (T1590). Moreover, information about hardware, software, operating system and programming languages can also be obtained via T1592. To gather such information efficiently and quickly, phishing technique (T1598) can be used in conjunction with other techniques. In order to get more information, searching of publicly available databases, social media platforms and websites (T1593, T1594 and T1596) should be searched. Such hunting for information is sometimes proved to be very fruitful. As an example, a password 1111111 of BWMS was found on social media platform that was uploaded by a crew member of the ship [50]. Whenever possible, active vulnerability scanning (T1595) can be used to gain further insight about the target.

After reconnaissance phase, next step is Resource Development (TA0042) which is important for later stages of the attack, especially for Initial Access (TA0001) and Persistence (TA0003). Relevant ATT&CK techniques under TA0042 are tabulated in Table 4.

Af first, to develop the staging capabilities (T1608), techniques T1650 and T1584 can be used to acquire information about network access and system infrastructure, respectively. An attacker can buy or obtain access to a target system or network by a number of secret web services and Initial Access Broker (IAB) networks. Infrastructure that can be utilized for targeting may be purchased, leased, or rented by an attacker. There are many different types of infrastructure available for hosting and managing adversarial activities. Domains, physical or cloud servers and third-party web services are examples of infrastructure solutions. Renting and buying botnets are additional options. Similarly, techniques T1584 and T1586 can be used to compromise infrastructure and accounts. For example, using these techniques a vulnerability CVE-2018-5071 was identified on Cobham Sea Tel satellite communication system devices. It was found that persistent cross-site scripting (stored XSS) [51] attack was possible in the web server of satellite communication devices that allowed remote attackers to inject malicious JavaScript code using the device's TELNET shell built-in commands. Some other known vulnerabilities present in marine satellite communication devices are CVE-2013-6034 and CVE-2013-6035. In CVE-2013-6034, it is mentioned that the firmware on Inmarsat, Japan Radio JUE-250 and JUE-500 and Thuraya IP satellite terminals has hardcoded credentials that makes it soft target for an attacker to extract unspecified login details form it. Moreover, these satellite terminals do not require authentication for sessions on TCP port 1827 that allows remote attackers to execute malicious codes (CVE-2013-6035). Finally, to strengthen the staging capabilities (T1608), additional malwares and exploits can be developed (T1587) beforehand to initiate later stages of the attack.

Table 5 MITRE ATT&CK Initial Access (TA0108) techniques

Technique ID	Technique for Initial Access
T0865	Spearphishing Attachment
T0866	Exploitation of Remote Services
T1078	Valid Accounts

After compromising the satellite communication system of the target ship, next action plan is to gain initial access (TA0108) to onboard network systems, persistence (TA0110) and then lateral movement (TA0109) toward BWMS. Because ship network is hybrid of IT and OT technologies, combination of ATT&CK techniques from Enterprise matrix and ICS matrix are required (Table 5). Moreover, to be successful for TA0108, an attacker can iterate between TA0043 and TA0042 tactics as shown in Fig. 1.

Initially, a spearphishing attachment (T0865) may be used to launch a social engineering attack on a particular target. Untrained crew member can be selected as a target for this purpose. All spearphishing techniques use electronic delivery of malware to gain access (TA0108) or privilege escalation (TA0111). Moreover, an attacker can exploit (T0866) a software or network vulnerability. For example, a fundamental problem is that the default accounts (T1078) like "admin", "administrator", "user" or "root" and passwords like "password", "admin", "user" or "12345", etc. for software or network devices are not changed at the time of commissioning of the ship [52, 53].

A natural way to proceed for the next phases of the attack is to do lateral movement (TA0109) through IT and OT sys-

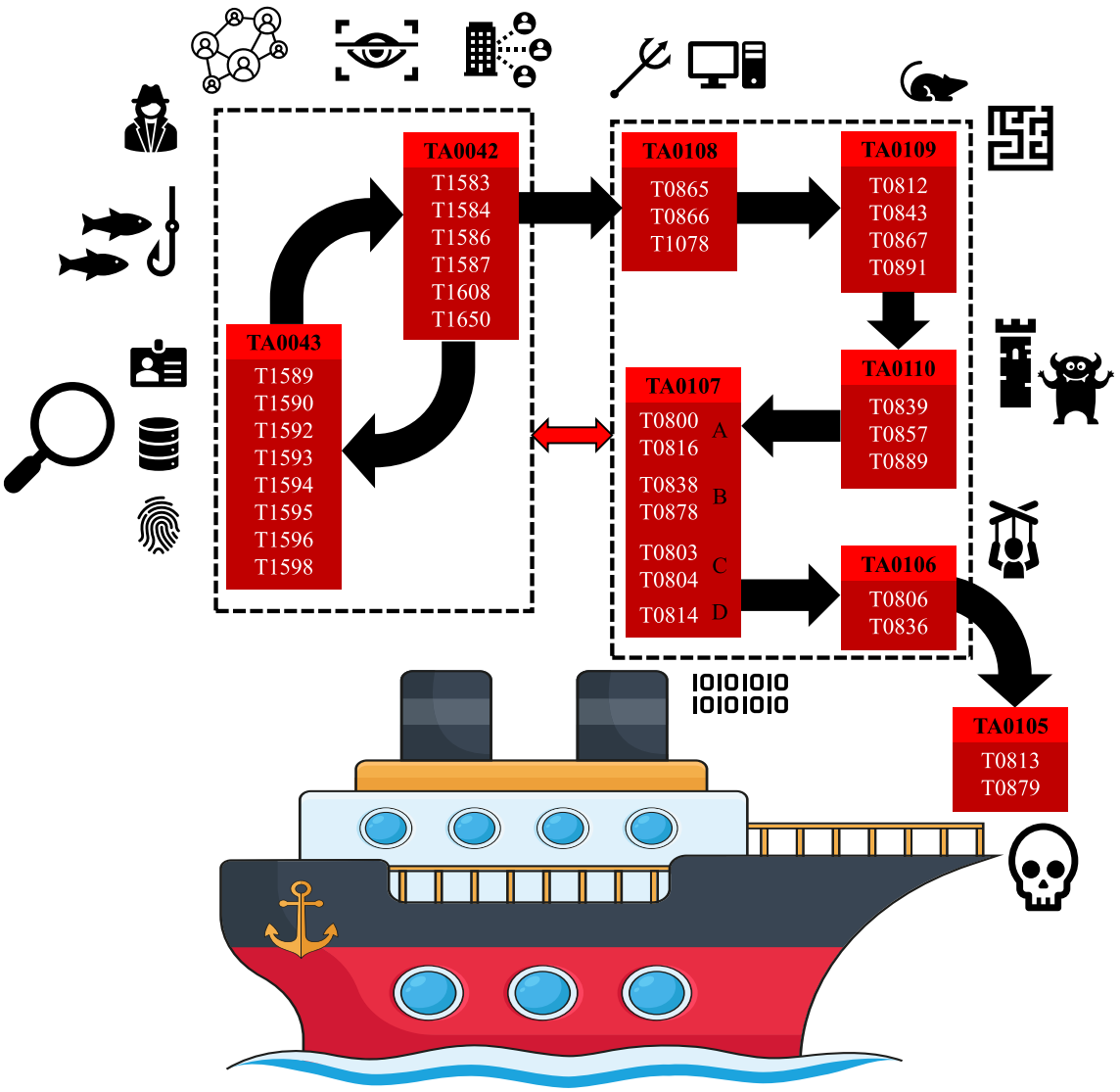

Fig. 1 MITRE ATT&CK tactics and techniques for sinking of ship

Table 6 MITRE ATT&CK Lateral Movement (TA0109) techniques

Technique ID	Technique for Lateral Movement
T0812	Default Credentials
T0843	Program Download
T0867	Lateral Tool Transfer
T0891	Hardcoded Credentials

Table 7 MITRE ATT&CK Persistence (TA0110) techniques

Technique ID	Technique for Persistence
T0839	Module Firmware
T0857	System Firmware
T0889	Modify Program

tems of the target ship. TA0109 comprises of techniques (Table 6) that an attacker can use to enter and remotely control the systems (devices) of the ship. These techniques can abuse default credentials (T0812) and hardcoded credentials (T0891) of devices and systems that are connected with both the IT and OT networks. Default and hardcoded credentials of devices (e.g., wind sensor) are normally provided in the technical specifications documents and most often they cannot be changed [54]. Moreover, the adversary can use lateral tool transfer (T0867) technique to pivot itself in a position where it should be able to transfer malicious tools from one point in a network to any other suitable point, without detection by possible intrusion detection system installed on a ship. During TA0109, it is important to maintain attack persistence (TA0110) for which techniques mentioned in Table 7 can be employed. Finally, after achieving a suitable vantage point, malicious programs can be downloaded (T0843) to the ship controllers that are controlling the BWMS of the target ship.

After TA0109, an attacker has reached to a position where it can cause significant damage to the ship. But before launching the decisive attack on BWMS of the ship, the goal is to paralyze the initial response system of the ship which triggers whenever abnormal functioning of OT systems is detected. Paralyzing the initial response systems further decreases the chances of detection. To inhibit the initial response to abnormalities, Inhibit Response Function (TA0107) techniques can be used, which are tabulated in Table 8.

An attacker has following four options to paralyze the response functions of the ship:

- *Option - A* An attacker can activate the firmware update mode of devices. Normally, a device in update mode does not respond or function as expected until the update is complete. And a device can be kept in an inactive holding state until the required firmware is not provided to it. Therefore, an attacker can paralyze the device by activating firmware update mode (T0800) and putting it in inactive state by not providing it the firmware update. An alternative to this approach is to force a device to shutdown or restart (T0816) multiple times.
- *Option - B* An attacker can disable the alarm system (T0878) of the ship to prevent alerting of operators present on the ship. Methods to prevent outgoing alarms from being raised and prevent incoming alarms from being responded to can involve tempering in the code memory of alarm system or modification of alarm settings (T0838). One important caveat is that suppression of alarm system may not result disabling of reporting system. Reporting system may still keep working in the background. To obstruct the reporting system, Option - C can be adopted along with Option - B.
- *Option - C* An attacker can prevent outgoing command messages (T0803) to reach to its destined devices. Similarly, an attacker can opt to block incoming reporting messages (0804) to reach at historian and reporting system.
- *Option - D* To paralyze the response system of a ship, an attacker can opt for traditional MiTM or denial of service attacks (T0814) in which the target device can be overloaded with a high volume of requests within a short time span or every packet of response messages can be dropped or spoofed.

Table 8 MITRE ATT&CK Inhibit Response Function (TA0107) Techniques

Technique ID	Technique for Inhibit Response Function	Option
T0800	Activate Firmware Update Mode	A
T0816	Device Restart/Shutdown	
T0838	Modify Alarm Settings	B
T0878	Alarm Suppression	
T0803	Block Command Message	C
T0804	Block Reporting Message	
T0814	Denial of Service	D

Lastly, in order to sink a ship, the final task is to flood the BWMS of the ship. BWMS is connected with PLCs controlled valves. To take control of these valves and to flood

Table 9 MITRE ATT&CK Impair Process Control (TA0106) techniques

Technique ID	Technique for Impair Process Control
T0806	Brute Force I/O
T0836	Modify Parameter

Table 10 MITRE ATT&CK Impact (TA0105) techniques

Technique ID	Technique for Impact	Mapping
T0813	Denial of Control	Operators are unable to control the ship's BWMS
T0879	Damage to Property	Ship sinks or capsizes on its one side

BWMS with water, techniques tabulated in Table 9 under Impair Process Control (TA0106) can be used.

For T0806, information gathered during TA0042 and TA0043 phases of the attack is crucial. If the information is available about all the attack points (valves and sensors), then instead of brute force attacks, specific valves can be attacked to flood either port side tank or starboard side tank of the BWMS. If less information is available or an attacker is not sure about which valves are controlling the BWMS then range of I/Os can be attacked to impair the process functions. An alternative approach is to change the threshold (T0836) of level sensors of BWMS and turning on the specific valve if information about it is available.

After success of all the phases of attacks launched so far, attackers are able to monitor the impact (TA0105) of their attacks. From MITRE ATT&CK framework, following two techniques tabulated in Table 10 can be mapped to sinking of a ship as an impact of the attacks.

Modeling of maritime attack scenario with ATT&CK tactics and techniques is depicted in Fig. 1. As clear from this figure, lot of the techniques are required for reconnaissance (TA0043) and resource gathering (TA0042). Both TA0042 and TA0043 techniques pave the ways for undetected lateral movement (TA0109) and fulfillment of other objectives. Moreover, an attacker can switch back (red double-headed arrow) to TA0043 and TA0042 loop if it feels more information and tools are required for the accomplishment of other objectives like TA0108, TA0109, TA0110, TA0107 and TA0106. TA0105 simply represents the sinking of a ship.

6 Maritime defense

MITRE D3FEND is under active development, and it is being updated with new mitigation techniques. Unlike MITRE ATT&CK framework, it does not have separate matrices for Enterprise, Mobile and ICS. Therefore, for the sake of effective coverage, two different defense mechanisms are designed in the subsequent subsections. In the first subsection, defense based on D3FEND framework is developed, whereas defense based on knowledge base of ATT&CK mitigations is elaborated in the second subsection. In order to navigate between ATT&CK mitigations and D3FEND framework, mapping between them is provided by D3FEND team in [55].

6.1 Defense from D3FEND

Based on D3FEND framework, defense incorporated for ship safety is enumerated in the hierarchical manner as follows:

- *Model* Defense starts with modeling of the ship from defense point of view. It involves inventorying of all the assets including hardware, software and network components onboard ship along with all the associated data and configurations. Apart from inventorying, network mapping for all the physical links is done as well as ship network traffic policies are defined. Moreover, all the systems and assets are scanned for vulnerabilities and all the vulnerabilities are enumerated.
- *Harden* This tactic is used for hardening of the ship model. Rigorous configurations of all the systems (e.g., BWMS) hardware (valves, sensors, etc.), software (operation and control) and network (IT and OT) components are performed to reduce the attack surface. For the crew on board ship, biometric and certificate-based authentication schemes are employed. Strong password policies and multi-factor authentication are enforced for everyone on board. Moreover, user account permissions are applied based on the role of the crew member. Such credential hardening reduces the chances of successful insider attacks. Strong encryption techniques are utilized for all kinds of two-way communications between ship to ship or ship to SCC. Lastly, all the software and firmwares are updated before starting the operations of the ship.
- *Detect* This tactic is used to identify unauthorized access or activity on the systems. For this purpose, sandbox environment is provided for malware detonation (dynamic analysis). Moreover, D3FEND artifacts [56] like IP addresses and file hashes are analyzed for spotting the benign or malicious identifier. Reputation analysis of URLs and IP addresses, emails and instant messages is also important from detection perspective. Traditionally, a ship has huge physical-layer attack surface. Intruders can try to penetrate via VHF link of AIS or they can try to access the communication network via satellite link. Global navigation satellite system (GNSS) receivers provide additional and attractive physical-layer attack surface to the attackers. To reduce the attack surface, network traffic analysis techniques like Connection Attempt Analysis, Inbound Session Volume Analysis, Protocol Metadata Anomaly Detection and Remote Terminal Session Detection can be used.
  Similarly, for detection of system intrusions at OT network, verification of devices firmware as well as OS is required. Behavior analysis and monitoring of peripher-

als, sensors (e.g., level sensor of BWMS) and control systems (e.g., PLC) are also important for detection purpose. Endpoint Health Beacons [22, 57] are of paramount importance for all the sensors that transmit periodic information to the controllers. Secondly, process analysis techniques for monitoring of a running control process for certain behaviors and conditions should be able to indicate abnormal responses. This includes control script (e.g., Structured Text script) execution analysis, system call analysis and process spawn analysis. Lastly, user behavior analysis can be beneficial for detection of insider attacks, and for this purpose, techniques related to analysis of resource access pattern and session duration are important.

- *Isolate* After detect tactic is in place for enhancing the defense of the ship, isolation of executable resources and network resources can be achieved by defining the policies for executable programs and files. Policies related to allowing (file signature authentication) or blacklisting executable reduce the success of spearphishing attacks. Hardware-based process isolation can be done with the help of Input–Output Memory Management Unit (IOMMU) [58]. Moreover, unauthorized devices and peripherals are restricted to access IO ports of the system. Network segmentation and use of demilitarized zone (DMZ) can provide additional layer of security to OT resources. Lastly, network filtering restricts the network traffic from unauthorized and untrusted networks.
- *Deceive* To give the false sense of victory to intruders, intelligently designed honeypot can be used that lure attackers to deceptive OT and IT systems of the ship.
- *Evict* For eviction, all the possible techniques are important because if an intruder has established the foothold in the system then it indicates that he is strong enough and possess all the necessary skills to cause serious harms to the ship. Therefore, once detected, removal of an adversary and its malicious assets should be of paramount importance and should be evicted as soon as possible.

From above discussions, it is clear that model, hardening, detection and eviction are mandatory, whereas isolation and deception tactics are complementary as they only raise the level of overall defense of a ship. All the defensive techniques considered for the security of the ship are marked with ✓ in Fig. 2.

6.2 Defense from ATT&CK mitigations

Defense by ATT&CK mitigations and in accordance with maritime attack (Fig. 1) is summed up in Table 11 and

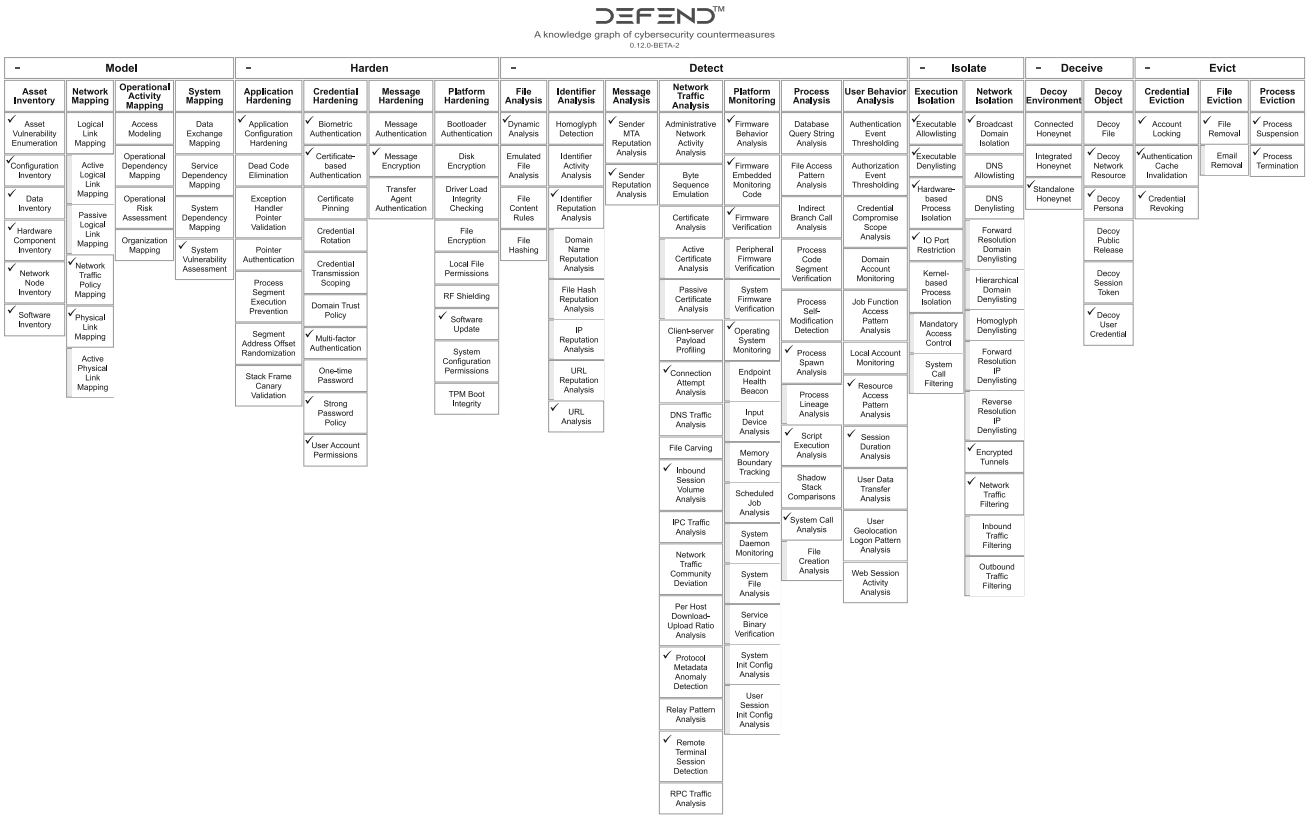

Fig. 2 MITRE D3FEND tactics and techniques [18, 22]

Table 11 MITRE ATT&CK mitigation techniques

Tactic ID	Technique ID	Mitigation ID	Mitigation
TA0043	T1589	M1056	Pre-compromise
	T1590		
	T1592		
	T1593	M1047	Audit
	T1594	M1056	Pre-compromise
	T1595		
	T1596		
	T1598	M1054	Software Configuration
		M1017	User Training
TA0042	T1583	M1056	Pre-compromise
	T1584		
	T1586		
	T1587		
	T1608		
	T1650		
TA0108	T0865	M0949	Antivirus/Antimalware
		M0931	Network Intrusion Prevention
		M0917	User Training
	T0866	M0948	Application Isolation and Sandboxing
		M0930	Network Segmentation
		M0951	Update Software
		M0950	Exploit Protection
	T1078	M1027	Password Policies
		M1026	Privileged Account Management
		M1017	User Training
TA0109	T0812	M0801	Access Management
		M0927	Password Policies
	T0843	M0801	Access Management
		M0947	Audit
		M0800	Authorization Enforcement
		M0937	Filter Network Traffic
		M0930	Network Segmentation
		M0813	Software Process and Device Authentication
	T0867	M0931	Network Intrusion Prevention
	T0891	M0801	Access Management
TA0110	T0839 T0857	M0946	Boot Integrity
		M0945	Code Signing
		M0802	Communication Authenticity
		M0808	Encrypt Network Traffic
		M0937	Filter Network Traffic
		M0807	Network Allowlists
		M0951	Update Software
	T0889	M0947	Audit
TA0107	T0800 T0816	M0801 M0800	Access Management Authorization Enforcement
	T0838	M0813	Software Process and Device Authentication
	T0878	M0810	Out-of-Band Communications Channel
	T0803	M0814	Static Network Configuration
	T0804	M0807	Network Allowllists
	T0814	M0815	Watchdog Timers
TA0106	T0806	M0813	Software Processes and Device Authentication
		M0937	Filter Network Traffic
	T0836	M0818	Validate Program Inputs
TA0105	T0813	M0811	Redundancy of Service
	T0879	M0812	Safety Instrumented Systems

detailed in this subsection. For the sake of brevity, defense from ATT&CK mitigations is presented succinctly without sacrificing the depth of analysis. To provide defense against ATT&CK tactics TA0042 and TA0043, crew on board ship must have adequate but maritime specific cybersecurity trainings (M1017, M0917) depending upon the rank of a crew member [59]. In addition to crew trainings, practice of auditing (M1047) must be in place for all onboard ship systems, policies, permissions and configurations (M1054). For OT systems, audit (M0947) must involve periodic checking of integrity of firmwares and controller codes as well as monitoring of events like device reboots or shutdown. Efforts should also be considered for protecting the secrecy of data associated with crew members. Availability of data should be minimized or prohibited for all sort of external parties (M1056).

To provide layers of protection against TA0108, TA0109 and TA0110 tactics, necessary crew trainings and auditing of all the systems are as important as necessary for TA0042 and TA0043 tactics. Secondly, all kinds of digital artifacts available at each layer of architecture (Purdue [60]) of the ship must be up-to-date (M0951) before starting the operations of the ship. Moreover, antivirus or antimalware softwares (M0949), exploit protection (M0950) and intrusion detection and prevention systems (M0931) must be placed at appropriate level of hierarchical architecture [60, 61]. Thirdly, policies for account management (M1026), access management (M0801) and passwords (M0927) must be defined at administrative level with enforced authorization (M0800) at every level of ship's systems and network architecture. Finally, the use of network filtering (M0937) for ingress or egress traffic or protocol-based filtering is required for protection against broad spectrum of network threats. Endpoint configurations for filtering of network packets are also mandatory. Encryption of network traffic (M0808) provides additional security. Network allowlisting or denylisting (M0807) specifies what connections (IP addresses, MAC addresses, ports, protocols) can be made from a device to network and vice versa. Mitigations like M0937, M0807, M0808 can be implemented with the help of deep-packet inspection (DPI) firewalls or context-aware firewalls, whereas for OT networks, SCADA protocol-aware firewalls can be used [62].

Four different options for paralyzing the emergency response functions of the ship are discussed in Sect. 5 and summarized in Table 8. For protection against unauthorized activation of firmware update mode (T0800) of a device (Option-A), mitigation technique (M0800) should be imposed for all devices. All the devices should be properly configured for read, manipulate or execute privileges and only authenticated and approved users should have access to most critical devices for their maintenance and updates. To protect alarm systems and their settings (Option-B), mitigation techniques M0813 and M0810 are useful. Like other devices, alarm systems must have restricted access and should be protected. Moreover, a redundant or out-of-band communication channel must be available for critical alarm systems. Similarly, blockage of command and reporting messages (Option-C) can be mitigated with M0810, M0814 and M0807 mitigation techniques. Denial-of-service attacks (Option-D) can be mitigated with the help of watchdog timers (M0815) that ensures timely detection of unresponsiveness of vital systems of the ship.

For tactics TA0105 and TA0106, end point devices like valves and sensors, which are controlled by PLCs and connected with BWMS of the ship should validate the format and content of the inputs (M0818) to ensure that the received parameters are within intended operational range. Sensor values should also be checked for abnormalities and enforced through PLCs. If a problematic output of sensors or invalid inputs to devices are identified, every device should be capable to generate an alert for the malicious activities and should switch to a predetermined safe mode during the event. Finally, critical systems should be made redundant (M0811) so that a redundant and healthy system takes control from the infected device in case a system becomes unresponsive due to a malicious attack.

7 Discussion

7.1 Key findings

Application of MITRE ATT&CK and D3FEND frameworks for cyber attack and cyber defense, respectively, prove their practicality for modeling of multidimensional nature of modern cybersecurity scenarios. As mentioned in Sect. 2, ATT&CK has three matrices, namely 'enterprise' for IT, 'ICS' for OT and 'mobile' for mobile technologies. As demonstrated in Sect. 5, enterprise matrix can be used for IT systems, e.g., OS-based operator consoles inside navigational bridge of the ship. Similarly, ICS matrix can be utilized for OT systems like controllers and valves. Mobile matrix is not used in this research because it mainly deals with mobile devices and their OS (Android, iOS). Like enterprise and ICS, mobile matrix is domain specific. There are many techniques in all three ATT&CK matrices which have same names but they are different and associated with different matrices. For example, a technique called Process Injection is available in both enterprise matrix (enterprise ID: T1055) and mobile matrix (mobile ID: T1631) but they are different due to change of context and domain. Like IT, OT and mobile, maritime also represents different but an important domain due to maritime specific systems and devices. We are not proposing to extend existing ATT&CK matrices because we argue that if an analyst uses existing ATT&CK matrices for maritime domain, it is difficult to truly reflect the gran-

ularity of cyber attack scenarios specific to maritime sector. Therefore, we intend to propose a new ATT&CK like matrix for maritime domain in future.

In Sect. 6, we have proposed two defense mechanisms for a ship. Based on our analysis, we can conclude that defense from D3FEND is proactive, whereas defense from ATT&CK mitigations is reactive. We argue that MITRE D3FEND is a proactive cyber defense framework that can be used to develop defensive strategies for proactively safeguarding maritime systems. We emphasize that D3FEND framework should be used for the development of a robust defensive strategies to mitigate potential exploitabilities and threats before they materialize. In contrast, ATT&CK mitigations are derived from real-world incidents of cyber attacks. It operates on the premise that by studying the tactics, techniques and procedures employed by cyber adversaries, effective defense strategies can be formulated. ATT&CK mitigations serve as valuable information and readily adaptable for maritime organizations seeking to strengthen their defenses based on known threat landscape, whereas D3FEND is more suitable for bolstering of defenses for unknown threat landscape.

Based on our synergistic work on maritime cyber attack and defense in Sects. 5 and 6, respectively, we suggest following basic but important recommendations: Firstly, training of on board crew is of utmost importance for cybersecurity of a ship. Importance of cybersecurity training for crew on board is also highlighted in [63], and it is mentioned in [64] that "80% of the cybersecurity incidents could have been prevented if single users were able to recognize the threat." Secondly, timely updates and proper configurations of all the IT and OT systems are also very important. Continuous patching and updates help getting rid of most of the vulnerabilities. Thirdly, all the physical USB, Ethernet and I/O ports must be blocked by physical port blockers as well as software port blockers. Fourthly, comprehensive incident response function and cyber risk management [65, 66] should be available on board ship. A ship should be kept in continuous cyber monitoring. Lastly, as mentioned in Sect. 3, IACS has adopted two new URs E26 and E27 [26] for cyber resilience of ship and its onboard systems and equipment, cybersecurity by design for a ship must also be enforced at an international level.

7.2 Strengths and limitations

MITRE ATT&CK framework is originally designed for enterprise, ICS and mobile, and it has not been used for maritime sector. For example, Dynamic Host Configuration Protocol (DHCP) spoofing (T1557.003) and Parent Process Identifier (PPID) spoofing (T1134.004) are available in ATT&CK, but there is no technique available for maritime GPS spoofing [67] and AIS spoofing [47]. Similarly, there are no techniques available for maritime RADAR and EDCIS systems. In Sect. 5, wherever appropriate ATT&CK technique is not available, we modeled the attack scenario with best possible closely related ATT&CK technique keeping in view the generalization of ATT&CK framework that it offers. As mentioned earlier, in future we intend to propose a MITRE ATT&CK like matrix specific to maritime sector.

MITRE ATT&CK matrices use high-level abstraction and do not directly provide in-depth details of implementation of cyber attack techniques, but it provides procedure examples for respective attack techniques in each ATT&CK matrix. For example, technique T0800 mentioned in Table 8 has one procedure example named Industroyer [68]. Through Tables 3, 4, 5, 6, 7, 8, 9 and 10, 35 techniques are mentioned in total and providing details of each attack technique could jeopardize the objective of this paper. Therefore, for sake of brevity and conciseness, we limited the scope of our analysis to higher-level details of MITRE ATT&CK. A higher-level abstraction allows us to address core requirements while keeping the overall system simple and more understandable.

7.3 Future work

Traditional ships are simple, and their functional components operate independent of each other. Rapid technological advancements are transforming traditional ships into remotely controlled ships and autonomous ships. Both remotely controlled ships and autonomous ships leverage the achievements of Artificial Intelligence (AI), hence increased telemetry and more interconnection among their intelligent systems. In future, we intend to model attacks on AI systems of autonomous ships using MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS) [69]. ATLAS is similar knowledge base to ATT&CK and D3FEND but is specific to AI systems. Similarly, we want to propose defense for AI systems of ship but MITRE D3FEND lacks the required elements for AI systems. Extension of D3FEND for AI systems is also considered as future work. Lastly, as mentioned in the previous subsection, three matrices of ATT&CK are related to IT, OT and mobile systems, we intend to propose a new maritime specific ATT&CK like matrix in future.

Risk management is beyond the scope of this work, but authors of this study are currently engaged in a research for the development of new kind of risk assessment framework for which Fig. 1 would be converted into Directed Cyclic Graph (DCG). The resulted DCG will be used as an input to the risk assessment framework for the calculations of risk ratings associated with IT, OT and AI systems of either traditional ships, remotely controlled ships or autonomous ships.

8 Conclusion

In this paper, an in-depth modeling of maritime attack scenario is performed with MITRE ATT&CK framework. As ATT&CK is based on real-world cybersecurity incidents, modeling with ATT&CK knowledge base is proven to be most realistic and suitable. Based on the developed ATT&CK model, we proposed a defense by leveraging ATT&CK mitigations, which predominantly serve as reactive measures to counteract and mitigate cyber threats as they emerge. Concurrently, we explored an alternative defense approach by incorporating MITRE D3FEND. It is determined that this framework emphasizes proactive measures. ATT&CK mitigation and D3FEND frameworks represent distinct approaches for incorporation of cyber defense, with D3FEND emphasizing proactive measures and ATT&CK mitigations taking a reactive and adaptive approach. D3FEND can be applied to a new ship or during the design phase of ship when a priori information of attack vector is unknown.

After modeling of attack and defense by ATT&CK and D3FEND, respectively, for a ship, it is identified that most of the elements of ATT&CK and D3FEND matrices are not specific to maritime systems. But keeping in view the generalization they offer, they can be used by making suitable assumptions or restricting the analysis to appropriate level of abstraction. However, due to the uniqueness of the maritime environment, we suggest creating separate matrices for maritime cyber attacks and defenses in future study.

Funding This research is supported by the National Research Foundation, Singapore (NRF) and Maritime and Port Authority of Singapore (MPA) under its Maritime Transformation Programme (Project No. SMI-2022-MTP-04). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of NRF and MPA.

Data availability Date sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare that they have no competing interest.

References

1. Outcome of the regulatory scoping exercise for the use of maritime autonomous surface ships (mass). https://www.imo.org/en/MediaCentre/PressBriefings/pages/MASSRSE2021.aspx, Accessed on July 14 (2023)
2. Zhou, X.Y., Liu, Z.J., Wang, F.W., Zhao Lin, W.: A system-theoretic approach to safety and security co-analysis of autonomous ships. Ocean Eng. **222**, 108569 (2021)
3. Initial sea trials successfully completed by wärtsilä & psa marine's ground-breaking 'intellitug' project. https://www.wartsila.com/media/news/13-03-2020-initial-sea-trials-successfully-completed-by-wartsila-psa-marine-s-ground-breaking-intellitug-project-3290931. Accessed 14 July 2023
4. Yara birkeland | yara international. https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/. Accessed 14 July 2023
5. Autonomous systems | l3harris® fast. forward. https://www.l3harris.com/all-capabilities/autonomous-systems. Accessed 14 July 2023
6. The nippon foundation meguri2040 fully autonomous ship program | the nippon foundation. https://www.nippon-foundation.or.jp/en/what/projects/meguri2040. Accessed 14 July 2023
7. Uncrewed surface vessel (usv) cetus: university of plymouth. https://www.plymouth.ac.uk/research/esif-funded-projects/usv-cetus. Accessed 14 July 2023
8. Autoferry - ntnu. https://www.ntnu.edu/autoferry. Accessed 14 July 2023
9. Rajaram, P., Goh, M., Zhou, J.: Guidelines for cyber risk management in shipboard operational technology systems. J. Phys.: Conf. Ser. **2311**, 012002 (2022)
10. Huang, B., Liu, Y.: A network vulnerability assessment method using general attack tree. In: 2022 5th International Conference on Data Science and Information Technology, DSIT 2022—Proceedings (2022)
11. Morikawa, I., Yamaoka, Y.: Threat tree templates to ease difficulties in threat modeling. In: Proceedings: 2011 International Conference on Network-Based Information Systems, NBiS 2011, pp. 673–678 (2011)
12. Khan, M.S., Siddiqui, S., Ferens, K.: A cognitive and concurrent cyber kill chain model. Comput. Netw. Secur. Essent. (2017). https://doi.org/10.1007/978-3-319-58424-9_34
13. Khan, R., McLaughlin, K., Laverty, D., Sezer, S.: Stride-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe 2017—Proceedings, 2018-January:1–6, 7 (2017)
14. Straub, J.: Modeling attack, defense and threat trees and the cyber kill chain, attck and stride frameworks as blackboard architecture networks. In: Proceedings: 2020 IEEE International Conference on Smart Cloud, SmartCloud 2020, pp. 148–153 (2020)
15. Bistarelli, S., Fioravanti, F., Peretti, P.: Defense trees for economic evaluation of security investments. In: Proceedings: First International Conference on Availability, Reliability and Security, ARES 2006(2006), pp. 416–423 (2006)
16. Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P.: Foundations of attack-defense trees. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 6561 LNCS, pp. 80–95 (2011)
17. Roy, A., Kim, D.S., Trivedi, K.S.: Attack countermeasure trees (act): towards unifying the constructs of attack and defense trees. Secur. Commun. Netw. **5**, 929–943 (2012)
18. Kaloroumakis, P.E., Smith, M.J.: Toward a knowledge graph of cybersecurity countermeasures. The MITRE Corporation, Case 20-2034 (2021)
19. Mitre att&ck®. https://attack.mitre.org/. Accessed 14 July 2023
20. Welcome to the cyber analytics repository | mitre cyber analytics repository. https://car.mitre.org/. Accessed 14 July 2023
21. Introduction to stix. https://oasis-open.github.io/cti-documentation/stix/intro.html. Accessed 14 July 2023
22. D3fend matrix | mitre d3fend™. https://d3fend.mitre.org/. Accessed 14 July 2023
23. Karim, M.S.: Maritime cybersecurity and the imo legal instruments: Sluggish response to an escalating threat? Mar. Policy **143**, 105138, 9 (2022)
24. Imo international convention for the safety of life at sea (solas) 1974. UN Treaty Series 1974, MSC.519(106), 11 (2022)

25. Msc 98-23-add.1 - report of the maritime safety committee on its ninety-eighth session (secretariat). https://www.imo.org. Accessed 14 July 2023
26. Iacs adopts new requirements on cyber safety - e26 and e27. https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/. Accessed 14 July 2023
27. Luh, R., Eresheim, S., Grosbacher, S., Petelin, T., Mayr, F., Tavolato, P., Schrittwieser, S.: Penquest reloaded: A digital cyber defense game for technical education. IEEE Global Engineering Education Conference, EDUCON, 2022-March:906–914 (2022)
28. Kaiser, F.K., Andris, L.J., Tennig, T.F., Iser, J.M., Wiens, M., Schultmann, F.: Cyber threat intelligence enabled automated attack incident response. In: Proceedings: 3rd International Conference on Next Generation Computing Applications, NextComp 2022 (2022)
29. Aghamohammadpour, A., Mahdipour, E., Attarzadeh, I.: Architecting threat hunting system based on the DODAF framework. J. Supercomput. **79**, 4215–4242, 3 (2023)
30. Benedetti, G., Verderame, L., Merlo, A.: Alice in (software supply) chains: risk identification and evaluation. Commun. Comput. Inf. Sci. **1621 CCIS**, 281–295 (2022)
31. Sikos, L.F.: Cybersecurity knowledge graphs. Knowledge and Information Systems, pp. 1–21 (2023)
32. Lund, M.S., Hareide, O.S., Jøsok, Ø.: An attack on an integrated navigation system. Necesse **3**(2), 149–163 (2018)
33. Lund, M.S., Gulland, J.E., Hareide, O.S., Josok, E., Weum, K.O.C.: Integrity of integrated navigation systems. In: 2018 IEEE Conference on Communications and Network Security, CNS 2018, 8 (2018)
34. Svilicic, B., Brčić, D., Žuškin, S., Kalebić, D.: Raising awareness on cyber security of ECDIS. Int. J. Mar. Navig. Saf. Sea Transp. **13**(1), 231–236 (2019)
35. Svilicic, B., Rudan, I., Frančić, V., Doričić, M.: Shipboard ECDIS cyber security: third-party component threats. Pomorstvo **33**(2), 176–180 (2019)
36. Svilicic, B., Rudan, I., Jugović, A., Zec, D.: A study on cyber security threats in a shipboard integrated navigational system. J. Mar. Sci. Eng. **7**, 364 (2019)
37. Nessus: vulnerability scanning tool. https://www.tenable.com/. Accessed 14 July 14 2023
38. Amro, A., Gkioulos, V.: From click to sink: Utilizing ais for command and control in maritime cyber attacks. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 13556 LNCS, pp. 535–553 (2022)
39. Svilicic, B., Kamahara, J., Rooks, M., Yano, Y.: Maritime cyber risk management: an experimental ship assessment. J. Navig. **72**, 1108–1120 (2019)
40. Cwe: common weakness enumeration. https://cwe.mitre.org/. Accessed 14 July 2023
41. Cve: common vulnerabilities and exposures. https://cve.mitre.org. Accessed 14 July 2023
42. Ahmed, A., Vasileios, G., Sokratis, K.: Assessing cyber risk in cyber-physical systems using the att&ck framework. ACM Trans. Priv. Secur. **26**(2), 1–33 (2021)
43. Iec 60812 ed. 3.0 b:2018—failure modes and effects analysis (fmea and fmeca). https://webstore.ansi.org/standards/iec/iec60812ed2018?gclid=EAIaIQobChMIg9PTzIyS_gIVYZlmAh3APQdPEAAYASAAEgILdvD_BwE. Accessed 14 July 2023
44. Oruc, A., Amro, A., Gkioulos, V.: Assessing cyber risks of an ins using the mitre att&ck framework. Sensors **22**, 8745 (2022)
45. Longo, G., Russo, E., Armando, A., Merlo, A.: Attacking (and defending) the maritime radar system. IEEE Trans. Inf. Forens. Secur. **18**, 3575–3589 (2023)
46. Longo, G., Merlo, A., Armando, A., Russo, E.: Electronic attacks as a cyber false flag against maritime radars systems. In: IEEE Proceedings—48th Conference on Local Computer Networks, LCN 2023, pp. 1–6 (2023)
47. Silverajan, B., Ocak, M., Nagel, B.: Cybersecurity attacks and defences for unmanned smart ships. pp. 15–20 (2018)
48. Secret files show alleged iranian plans to sink ships using cyberattacks | the times of israel. https://www.timesofisrael.com/secret-files-show-alleged-iranian-plans-to-sink-ships-using-cyberattacks/. Accessed 14 July 2023
49. International convention for the control and management of ships' ballast water and sediments (bwm). https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Control-and-Management-of-Ships%27-Ballast-Water-and-Sediments-(BWM).aspx. Accessed 14 July 2023
50. Jo, Y., Choi, O., You, J., Cha, Y., Lee, D.H.: Cyberattack models for ship equipment based on the mitre att&ck framework. Sensors **22**, 1860 (2022)
51. What is persistent xss | acunetix. https://www.acunetix.com/blog/articles/persistent-xss/. Accessed 14 July 2023
52. Timm, C., Perez, R.: Seven deadliest social network attacks. Seven Deadliest Social Network Attacks (2010)
53. York, D.: Seven deadliest unified communications attacks. Seven Deadliest Unified Communications Attacks (2010)
54. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A.: Nist special publication 800-82 revision 2 guide to industrial control systems (ics) security supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc)
55. Att&ck mitigations to d3fend mappings | mitre d3fend^{TM}. https://d3fend.mitre.org/mappings/attack-mitigations/. Accessed 14 July 2023
56. Digital artifact ontology | mitre d3fend^{TM}. https://d3fend.mitre.org/dao/. Accessed 14 July 2023
57. Ray, K.D.: Intrusion detection using a heartbeat, 4 (2023)
58. Kornaros, G., Harteros, K., Christoforakis, I., Astrinaki, M.: I/o virtualization utilizing an efficient hardware system-level memory management unit. 2014 International Symposium on System-on-Chip, SoC 2014, 12 (2014)
59. BIMCO and ICS Witherbys. Cyber Security Workbook for On Board Ship Use - 4th Edition, 2023 - Witherbys. 4th edition, 10 (2022)
60. Williams, T.J.: The purdue enterprise reference architecture. IFAC Proc. Vol. **26**, 559–564, 7 (1993)
61. Yousaf, A., Loan, A., Babiceanu, R.F., Maglaras, L., Yousaf, O.: Convergence of detection probability, computational gains, and asymptotic analysis of an algorithm for physical-layer intrusion detection system. Trans. Emerg. Telecommun Technol. **29**(8), e3430 (2018)
62. Li, D., Guo, H., Zhou, J., Zhou, L., Wong, J.W.: Scadawall: a cpi-enabled firewall model for scada security. Comput. Secur. **80**, 134–154, 1 (2019)
63. Bothur, D., Zheng, G., Valli, C.: A critical analysis of security vulnerabilities and countermeasures in a smart ship system. In: 15th Australian Information Security Management Conference, pp. 81–87 (2017)
64. Zăgan, R., Raicu, G.: Understanding of the cyber risk on board ship and ship stability. Annals of "Dunarea de Jos" University of Galati. Fascicle XI Shipbuild. **42**, 81–90, 11 (2019)
65. Kavallieratos, G., Spathoulas, G., Katsikas, S.: Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems. Sensors **21**, 1691 (2021)

66. Kavallieratos, G., Katsikas, S.: Managing cyber security risks of the cyber-enabled ship. J. Mar. Sci. Eng. **8**, 768 (2020)
67. Bhatti, J., Humphreys, T.E.: Hostile control of ships via false gps signals: demonstration and detection. Navigation **64**, 51–66, 3 (2017)
68. Kozak, P., Klaban, I., Slajs, T.: Industroyer cyber-attacks on ukraine's critical infrastructure. In: 2023 9th International Conference on Military Technologies, ICMT 2023—Proceedings (2023)
69. Mitre | atlas^{TM}. https://atlas.mitre.org. Accessed 22 Oct 2023

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.